APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/796,932	03/09/2004	Akio Sakamoto	60054-0016	3286

			EXAMINER
29989	7590	08/23/2006	VAUTROT, DENNIS L

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

ART UNIT	PAPER NUMBER
2167	

DATE MAILED: 08/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	10/796,932	SAKAMOTO ET AL.
	Examiner	Art Unit	
	Dennis L. Vautrot	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>09 March 2004</u>.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-30</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1-30</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on <u>09 March 2004</u> is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some *   c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>11/17/05, ... 9/7/2004 and 5/3/2004</u>

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1.   The information disclosure statements (IDS) submitted on 17 November 2005, 26

July 2005, 7 September 2004, and 3 May 2004 have been received and entered into the

record. Since the IDS comply with the provisions of MPEP § 609, the references cited

therein have been considered by the examiner. See attached forms PTO-1449.

Claim Rejections - 35 USC § 101

2.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of
> matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the
> conditions and requirements of this title.

Claims 15-28 are rejected under 35 U.S.C. 101 because the claimed invention is

directed to non-statutory subject matter. In the specification on page 30, transmission

media is defined to include acoustic or light waves, radio-waves and infra-red data

communications. According to Annex IV of the "Interim Guidelines for Examination of

Patent Applications for Subject Matter Eligibility" that was signed on October 26, 2005

and posted at http://www.uspto.gov/web/offices/pac/dapp/ogsheet.html, these are

considered to be nonstatutory subject matter because it does not fall into any of the four

statutory classes of invention.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4.   Claims 1 – 14, 29 and 30 are rejected under 35 U.S.C. 102(b) as being

anticipated by **Sekiguchi** (EP 0 999 490 A2).

5.   Regarding claim 1, **Sekiguchi** teaches a method for monitoring a database,

comprising: collecting user behavior data [access log] that indicates how one or more

users use the database (See column 4, paragraph [0021] "the access monitor unit 10

acquires an access log using an access log acquisition unit 11"); processing and storing ·

the data as historical data (See column 4, paragraph [0021] where the obtained access

log represents the stored historical data.); analyzing the historical data to determine

behavior patterns [security management information] (See column 4, paragraph [0020]

"executes the statistical process of the access log using a security management unit,

and stores the obtained result as security management information."); receiving a new

set of data [access log] that indicates how one or more users have used the database

(See column 4, paragraph [0021] "the access monitor unit 10 acquires an access log

using an access log acquisition unit 11"); performing a comparison between the new set

of data [access log] and the behavior pattern [security management information] (See

column 4, paragraph [0021] "...comparing the access log acquired by the access log

acquisition unit 11 with security management information obtained from the access log

in the past using a security check unit 14."); determining based on the comparison,

whether the new set of data [access log] satisfies a set of criteria [access restriction]

(See column 4, paragraph [0022] "...the access log and the security management

information are compared using the security check unit 14. If the access log of this time

violates the set access restriction..."); if the new set of data satisfies the set of criteria,

then determining that the new set of data represents anomalous activity (See column 4,

paragraph [0021] "...and judges that an access gained in a situation different from a

normal one is an abnormal access..."); and responding to the determination by

performing a targeted operation [issuing an alarm] (See column 4, paragraph [0022]

"...and issues an alarm to the manager or specific user using the abnormality alarm unit

20.")

6.   Regarding claim 2, **Sekiguchi** teaches determining if the new set of data [access

log] violates a rule based policy [access restriction information]; and if the new set of

data violates the rule based policy, then determining that the new set of data represents

anomalous activity. (See column 5, lines 54 – column 6, line 6 "...an access restriction

setting unit 113 for setting access restriction information 204 which defines conditions

for detecting abnormality, and a security check unit 114 for checking whether access is

normal. The security check unit 114 includes ... a restriction comparison unit 116 for

judging whether access violates the set access restriction information 204.")

7.   Regarding claim 3, **Sekiguchi** teaches collecting user behavior data further

comprises: reading information from an audit trail or dynamic performance views of the

database manager. (See column 6, paragraph [0029] "For an access log 201,

information, such as the name of a user, a password, the data and time of an access,

the name of an accessed file, the name of an executed command, etc., are acquired

and stored." The dynamic performance views description in the instant application's

specification in paragraph [0009] refers to information on current db usage and resource

utilization, which is what is represented by the quote in the reference with date and time

of an access, the name of an accessed file, etc.)

8.   Regarding claim 4, **Sekiguchi** teaches collecting user behavior data further

comprises collecting information at a monitoring level selected from at least one of:

information about database access for one or more selected database objects [file] (See

column 6, paragraph [0030] "Alternatively, the access log 201 can be statistically

processed for each file or computer and can be stored as security management

information 203."); information about database access for one or more selected

database users (See column 6, paragraph [0030] "converts the access log to security

management information 203, such as...for each user, and stores obtained

information.") and information about database access for one or more selected

database user sessions.

9.   Regarding claim 5, **Sekiguchi** teaches collecting user behavior data further

comprises: receiving a type of information [contents to be compared] to be monitored;

(See column 7, paragraph [0036] "The contents to be compared can be set in advance

by a user or can be determined by a manager. Alternatively, modifications can be made

according to the desired level of security."); determining a monitoring level [In this case,

user] from the type of information; and activating audit options [storing executed

commands of user A] of the database manager based upon the monitoring level

determined. (See column 7, paragraph [0037] "It is assumed here that the date and

time of an access, accessed file and executed command of a user A are managed for

the purpose of security, and the information is compared with the acquired access log in

order to judge whether this access is within the scope of the security management

information 203." Here, the monitoring level would be user, based on the type of

information – date, time, accessed file, executed commands of user A." For user level

auditing, statement auditing for a specific user is enabled, as mentioned in the instant

applications specification [0061] explains activating audit options of the database

manager.)

10.   Regarding claim 6, **Sekiguchi** teaches analyzing the historical data to determine

behavior patterns further comprises: determining a statistical model from the historical

data. (See column 6, paragraph [0030] "The security management unit 112 executes

the statistical process of the access log 201 which is acquired by the access log

acquisition unit 111...")

11.   Regarding claim 7, **Sekiguchi** teaches determining a statistical model from the

historical data further comprises: determining a frequency of database access from the

historical data [access log] (See column 6, paragraph [0030] "...converts the access log

to security management information 203, such as the frequency of access...");

determining a probability function [statistical process] for frequencies of database

access (See column 7, paragraph [0035] "For this reason, the security management unit

112 manages information about a time zone using a method for determining the scope

of the time zone where access is gained with a statistical process."); and determining a

cumulative probability function from the probability function (See column 7, paragraph

[0035] "Such statistical information about an access is calculated for all accesses

without dividing a section or by dividing a section of, for example, the past one month or

one year, if necessary, and the time zone in which an access is permitted is set based

on the calculation.")

12.   Regarding claim 8, **Sekiguchi** teaches performing a comparison between the

new set of data [access log] and the behavior pattern [security management

information] further comprises: testing a hypothesis using the new set of data [access

log] against the statistical model [process] (See column 6, paragraph [0030] "The

security management unit 112 executes the statistical process of the access log 201

which is acquired by the access log acquisition unit 111, converts the access log to

security management information 203....").

13.   Regarding claim 9, **Sekiguchi** teaches testing a hypothesis using the new set of

data against the statistical model further comprises: determining a frequency of

database access for the new set of data [access log] (See column 6, paragraph [0030]

"converts the access log to security management information, such as the frequency of

access to the file..."); and determining the threshold value [scope of the time zone] from

a guard criteria [plus/minus 3s] and a probability function parameter [statistical process]

(See column 7, paragraph [0035] "For this reason, the security management unit 112

manages information about a time zone using a method for determining the scope of

the time zone where access is gained with a statistical process...a time zone from

which a user access is judged to be normal is assumed to be a scope of plus/minus

3s... If this method is adopted, the access time zone of a user automatically changes

according to the use situation of the user, regardless of its initial setting, thus making it

convenient.")

14.   Regarding claim 10, **Sekiguchi** teaches testing a hypothesis using the new set of

data [access log] against the statistical model pattern [security management

information] further comprises: comparing the frequency of database access [included

in the access log] for the new set of data [access log] with the threshold value [access

situation] (See column 7, paragraph [0036] "A log comparison unit 115 compares the

access log 201 of this time which is acquired by the access acquisition unit 111 with the

access situation of security management information 203 which is acquired from log

information acquired before.")

15.   Regarding claim 11, **Sekiguchi** teaches the historical information is about

database access for one or more selected database objects and wherein determining a

frequency of database access from the historical data [access log] further comprises

determining a frequency of at least one of: object access frequency by hour of day

[access date and time], object access frequency by hour of day and operating system

user, object access frequency by hour of day and database user, object access

frequency by hour of day and location, object access frequency by hour of day and

combination of at least two of operating system user, database user and location. (See

column 6, paragraph [0030] "...the access log acquisition unit 111 converts the access

log to security management information 203, such as the frequency of access, the time

zone of access data and time... the name of a file accessed in the past, the frequency

of access to the file...Alternatively, the access log 201 can be statistically processed for

each file or computer, and can be stored as security management information 203.")

16.   Regarding claim 12, **Sekiguchi** teaches the historical information [access log] is

about database access for one or more selected database users and wherein

determining a frequency of database access from the historical data further comprises

determining a frequency of at least one of: user access frequency by hour of day

[access time], user access frequency by hour of day and operating system user [access

time and user A], user access frequency by hour of day and database user, user access

frequency by hour of day and location, user access frequency by hour of day and a

combination of at least two of operating system user, database user, and location. (See

column 8, paragraph [0039] "...if the access log 201 of the user A is as shown in Fig. 3

and the security management information 203 as shown in Fig 4 is stored for the user

A, the access time is 18:30:34...In this case the access is judged to be normal and it is

checked whether the access violates the access restriction.")

17.   Regarding claim 13, **Sekiguchi** teaches the historical information is about

database access for one or more selected database user sessions [access situation]

and wherein determining a frequency of database access from the historical data further

comprises determining a frequency of at least one of: number of page reads per session

[frequency of access], access duration per session [elapsed time], number of page

reads per unit time [frequency of access]. (See column 3, paragraph [0016] "modifying a

setting file to be used according to the access situation of a user, such as elapsed time,

the frequency of accesses etc., and modifying and managing a security level, can be

provided in order to manage the security level.")

18.   Regarding claim 14, **Sekiguchi** teaches performing a targeted operation

comprises at least one of: raising an alert [alarm]; sending an email; producing a report;

performing a visualization. (See column 4, paragraph [0020] "...alarm unit for issuing an

alarm and reporting to a manager or a specific user...")

19.   Regarding claim 29, **Sekiguchi** teaches an apparatus, comprising: means for

collecting user behavior data [access log] that indicates how one or more users use the

database (See column 4, paragraph [0021] "the access monitor unit 10 acquires an

access log using an access log acquisition unit 11"); means for processing and storing

the data as historical data (See column 4, paragraph [0021] where the obtained access

log represents the stored historical data.); means for analyzing the historical data to

determine behavior patterns [security management information] (See column 4,

paragraph [0020] "executes the statistical process of the access log using a security

management unit, and stores the obtained result as security management

information."); means for receiving a new set of data [access log] that indicates how

one or more users have used the database (See column 4, paragraph [0021] "the

access monitor unit 10 acquires an access log using an access log acquisition unit 11");

means for performing a comparison between the new set of data [access log] and the

behavior pattern [security management information] (See column 4, paragraph [0021]

"...comparing the access log acquired by the access log acquisition unit 11 with security

management information obtained from the access log in the past using a security

check unit 14."); means for determining based on the comparison, whether the new set

of data [access log] satisfies a set of criteria [access restriction] (See column 4,

paragraph [0022] "...the access log and the security management information are

compared using the security check unit 14. If the access log of this time violates the set

access restriction..."); if the new set of data satisfies the set of criteria, then determining

that the new set of data represents anomalous activity (See column 4, paragraph [0021]

"...and judges that an access gained in a situation different from a normal one is an

abnormal access..."); and means for responding to the determination by performing a

targeted operation [issuing an alarm] (See column 4, paragraph [0022] "...and issues an

alarm to the manager or specific user using the abnormality alarm unit 20.")

20.   Regarding claim 30, **Sekiguchi** teaches an apparatus, comprising:

        a data collector [access monitor unit] for collecting user behavior data [access

log] that indicates how one or more users use the database (See column 4, paragraph

[0021] "the access monitor unit 10 acquires an access log using an access log

acquisition unit 11"); processing and storing the data as historical data (See column 4,

paragraph [0021] where the obtained access log represents the stored historical data.);

receiving a new set of data [access log] that indicates how one or more users have

used the database (See column 4, paragraph [0021] "the access monitor unit 10

acquires an access log using an access log acquisition unit 11");

        a data analyzer [access monitor unit] for analyzing the historical data to

determine behavior patterns analyzing the historical data to determine behavior patterns

[security management information] (See column 4, paragraph [0020] "the access

monitor unit...executes the statistical process of the access log using a security

management unit, and stores the obtained result as security management

information."); and

an anomaly detector [access monitor unit] for performing a comparison between

the new set of data [access log] and the behavior pattern [security management

information] (See column 4, paragraph [0021] "The access monitor unit...comparing the

access log acquired by the access log acquisition unit 11 with security management

information obtained from the access log in the past using a security check unit 14.");

determining based on the comparison, whether the new set of data [access log]

satisfies a set of criteria [access restriction] (See column 4, paragraph [0022] "...the

access log and the security management information are compared using the security

check unit 14. If the access log of this time violates the set access restriction..."); if the

new set of data satisfies the set of criteria, then determining that the new set of data

represents anomalous activity (See column 4, paragraph [0021] "...and judges that an

access gained in a situation different from a normal one is an abnormal access..."); and

responding to the determination by performing a targeted operation [issuing an alarm]

(See column 4, paragraph [0022] "...and issues an alarm to the manager or specific

user using the abnormality alarm unit 20.")

Claim Rejections - 35 USC § 103

21.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

22.   Claims 15-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Sekiguchi in view of **Ho** (6,597,777).

23.   Regarding claim 15, **Sekiguchi** teaches a computer-readable medium carrying

one or more sequences of instructions when executed by one or more processors (See

column 3, paragraph [0017] ("...can be stored in an appropriate computer-readable

medium to execute each of the above described process..."), cause the one or more

processors to carry out the steps of: collecting user behavior data [access log] that

indicates how one or more users use the database (See column 4, paragraph [0021]

"the access monitor unit 10 acquires an access log using an access log acquisition unit

11"); processing and storing the data as historical data (See column 4, paragraph [0021]

where the obtained access log represents the stored historical data.); analyzing the

historical data to determine behavior patterns [security management information] (See

column 4, paragraph [0020] "executes the statistical process of the access log using a

security management unit, and stores the obtained result as security management

information."); receiving a new set of data [access log] that indicates how one or more

users have used the database (See column 4, paragraph [0021] "the access monitor

unit 10 acquires an access log using an access log acquisition unit 11"); performing a

comparison between the new set of data [access log] and the behavior pattern [security

management information] (See column 4, paragraph [0021] "...comparing the access

log acquired by the access log acquisition unit 11 with security management information

obtained from the access log in the past using a security check unit 14."); determining

based on the comparison, whether the new set of data [access log] satisfies a set of

criteria [access restriction] (See column 4, paragraph [0022] "...the access log and the

security management information are compared using the security check unit 14. If the

access log of this time violates the set access restriction..."); if the new set of data

satisfies the set of criteria, then determining that the new set of data represents

anomalous activity (See column 4, paragraph [0021] "...and judges that an access

gained in a situation different from a normal one is an abnormal access..."); and

responding to the determination by performing a targeted operation [issuing an alarm]

(See column 4, paragraph [0022] "...and issues an alarm to the manager or specific

user using the abnormality alarm unit 20.")

Sekiguchi fails to teach reverting to a recovery configuration in response to

device faults. However, Ho teaches reverting to a recovery configuration [corrective

module] in response to device faults [server failure]. (See column 11, lines 7-8 "Upon

the onset of a server failure, the failing service class unfairly ties up network resources",

lines 12-16 "The present invention, however, detects the fact that the traffic intensity

persistently exceeds the upper threshold within the first 15 minutes of the onset of the

server failure and detects the service class with which the failure is associated..." lines

26-32 "...one or more corrective control modules connecting detector 604 and network

601, may be responsive to a generated alarm for automatic corrective action...") It

would have been obvious to one with ordinary skill in the art at the time of the invention

to combine the teachings of Sekiguchi with that of Ho because they both deal with

monitoring networks and databases, and by including a way to handle device faults, the

medium becomes more robust than before, allowing faults to not disrupt the monitoring.

It is for this reason that one of ordinary skill in the art would have been motivated to

include revering to a recovery configuration in response to device faults.

24.   Regarding claim 16, **Sekiguchi** additionally teaches instructions which, when

executed by the one or more processors, cause the one or more processors to carry out

the steps of: determining if the new set of data [access log] violates a rule based policy

[access restriction information]; and if the new set of data violates the rule based policy,

then determining that the new set of data represents anomalous activity. (See column 5,

lines 54 – column 6, line 6 "…an access restriction setting unit 113 for setting access

restriction information 204 which defines conditions for detecting abnormality, and a

security check unit 114 for checking whether access is normal. The security check unit

114 includes … a restriction comparison unit 116 for judging whether access violates

the set access restriction information 204.")

25.   Regarding claim 17, **Sekiguchi** additionally teaches the instructions for carrying

out the step of collecting user behavior data further comprise instructions for carrying

out the step of: reading information from an audit trail of the database manager. (See

column 6, paragraph [0029] "For an access log 201, information, such as the name of a

user, a password, the data and time of an access, the name of an accessed file, the

name of an executed command, etc., are acquired and stored." The stored information

in the access log is the audit trail of the database manager.)

26.   Regarding claim 18, **Sekiguchi** additionally teaches collecting information at a

monitoring level selected from at least one of: information about database access for

one or more selected database objects [file] (See column 6, paragraph [0030]

"Alternatively, the access log 201 can be statistically processed for each file or

computer and can be stored as security management information 203."); information

about database access for one or more selected database users (See column 6,

paragraph [0030] "converts the access log to security management information 203,

such as...for each user, and stores obtained information.") and information about

database access for one or more selected database user sessions.

27.   Regarding claim 19, **Sekiguchi** additionally teaches collecting user behavior data

further comprise instructions for carrying out the steps of: receiving a type of information

[contents to be compared] to be monitored; (See column 7, paragraph [0036] "The

contents to be compared can be set in advance by a user or can be determined by a

manager. Alternatively, modifications can be made according to the desired level of

security."); determining a monitoring level [In this case, user] from the type of

information; and activating audit options [storing executed commands of user A] of the

database manager based upon the monitoring level determined. (See column 7,

paragraph [0037] "It is assumed here that the date and time of an access, accessed file

and executed command of a user A are managed for the purpose of security, and the

information is compared with the acquired access log in order to judge whether this

access is within the scope of the security management information 203." Here, the

monitoring level would be user, based on the type of information – date, time, accessed

file, executed commands of user A." For user level auditing, statement auditing for a

specific user is enabled, as mentioned in the instant applications specification [0061]

explain activating audit options of the database manager.)

28.   Regarding claim 20, **Sekiguchi** additionally teaches analyzing the historical data

to determine behavior patterns further comprise instructions for carrying out the step of:

determining a statistical model from the historical data. (See column 6, paragraph

[0030] "The security management unit 112 executes the statistical process of the

access log 201 which is acquired by the access log acquisition unit 111...")

29.   Regarding claim 21, **Sekiguchi** additionally teaches determining a statistical

model from the historical data further comprise instructions for carrying out the step of:

determining a frequency of database access from the historical data [access log] (See

column 6, paragraph [0030] "...converts the access log to security management

information 203, such as the frequency of access..."); determining a probability function

[statistical process] for frequencies of database access (See column 7, paragraph

[0035] "For this reason, the security management unit 112 manages information about a

time zone using a method for determining the scope of the time zone where access is

gained with a statistical process."); and determining a cumulative probability function

from the probability function (See column 7, paragraph [0035] "Such statistical

information about an access is calculated for all accesses without dividing a section or

by dividing a section of, for example, the past one month or one year, if necessary, and

the time zone in which an access is permitted is set based on the calculation.")

30.   Regarding claim 22, **Sekiguchi** additionally teaches performing a comparison

between the new set of data [access log] and the behavior pattern [security

management information] further comprise instructions for carrying out the step of:

testing a hypothesis using the new set of data [access log] against the statistical model

[process] (See column 6, paragraph [0030] "The security management unit 112

executes the statistical process of the access log 201 which is acquired by the access

log acquisition unit 111, converts the access log to security management information

203....").

31.   Regarding claim 23, **Sekiguchi** additionally teaches testing a hypothesis using

the new set of data against the statistical model further comprise instructions for

carrying out the steps of: determining a frequency of database access for the new set of

data [access log] (See column 6, paragraph [0030] "converts the access log to security

management information, such as the frequency of access to the file..."); and

determining the threshold value [scope of the time zone] from a guard criteria

[plus/minus 3s] and a probability function parameter [statistical process] (See column 7,

paragraph [0035] "For this reason, the security management unit 112 manages

information about a time zone using a method for determining the scope of the time

zone where access is gained with a statistical process...a time zone from which a user

access is judged to be normal is assumed to be a scope of plus/minus 3s... If this

method is adopted, the access time zone of a user automatically changes according to

the use situation of the user, regardless of its initial setting, thus making it convenient.")

32.   Regarding claim 24, **Sekiguchi** additionally teaches testing a hypothesis using

the new set of data against the statistical model further comprise instructions for

carrying out the step of: comparing the frequency of database access [included in the

access log] for the new set of data [access log] with the threshold value [access

situation] (See column 7, paragraph [0036] "A log comparison unit 115 compares the

access log 201 of this time which is acquired by the access acquisition unit 111 with the

access situation of security management information 203 which is acquired from log

information acquired before.")

33.   Regarding claim 25, **Sekiguchi** additionally teaches the historical information is

about database access for one or more selected database objects and wherein the

instructions for carrying out the step of determining a frequency of database access

from the historical data [access log] further comprise instructions for carrying out the

step of determining a frequency of at least one of: object access frequency by hour of

day [access date and time], object access frequency by hour of day and operating

system user, object access frequency by hour of day and database user, object access

frequency by hour of day and location, object access frequency by hour of day and

combination of at least two of operating system user, database user and location. (See

column 6, paragraph [0030] "...the access log acquisition unit 111 converts the access

log to security management information 203, such as the frequency of access, the time

zone of access data and time... the name of a file accessed in the past, the frequency

of access to the file...Alternatively, the access log 201 can be statistically processed for

each file or computer, and can be stored as security management information 203.")

34.   Regarding claim 26, **Sekiguchi** additionally teaches the historical information

[access log] is about database access for one or more selected database users and

wherein the instructions for carrying out the steps of determining a frequency of

database access from the historical data further comprise instructions for carrying out

the step of determining a frequency of at least one of: user access frequency by hour of

day [access time], user access frequency by hour of day and operating system user

[access time and user A], user access frequency by hour of day and database user,

user access frequency by hour of day and location, user access frequency by hour of

day and a combination of at least two of operating system user, database user, and

location. (See column 8, paragraph [0039] "...if the access log 201 of the user A is as

shown in Fig. 3 and the security management information 203 as shown in Fig 4 is

stored for the user A, the access time is 18:30:34...In this case the access is judged to

be normal and it is checked whether the access violates the access restriction.")

35.   Regarding claim 27, **Sekiguchi** additionally teaches the historical information is

about database access for one or more selected database user sessions [access

situation] and wherein the instructions for carrying out the step of determining a

frequency of database access from the historical data further comprise instructions for

carrying out the step of determining a frequency of at least one of: number of page

reads per session [frequency of access], access duration per session [elapsed time],

number of page reads per unit time [frequency of access]. (See column 3, paragraph

[0016] "modifying a setting file to be used according to the access situation of a user,

such as elapsed time, the frequency of accesses etc., and modifying and managing a

security level, can be provided in order to manage the security level.")

36.   Regarding claim 28, **Sekiguchi** additionally teaches performing a targeted

operation comprises comprise instructions for carrying out at least one of: raising an

alert [alarm]; sending an email; producing a report; performing a visualization. (See

column 4, paragraph [0020] "...alarm unit for issuing an alarm and reporting to a

manager or a specific user...")

Conclusion

37.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

   Mattson (EP 1 315 065 A1) teaches a method for intrusion detection in a

database system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dennis L. Vautrot whose telephone number is 571-272-2184. The examiner can normally be reached on Monday-Friday 8:30-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Cottingham can be reached on 571-272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Dv
8/17/2006

JOHN COTTINGHAM
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100